Addonics TECHNOLOGIES

User Guide

CipherUSB FDE

(CAUF1W, CAUF1W-2, CAUF1M, CAUF1M-2,
CAUF2W, CAUF2W-2, CAUF2M, CAUF2M-2)

www.addonics.com

Technical Support
If you need any assistance to get your unit functioning properly, please have your product information ready and contact Addonics Technical Support at:

Hours: 8:30 am - 6:00 pm PST
Phone: 408-453-6212
Email: http://www.addonics.com/support/query/

Overview

The CipherUSB works by encrypting data using a 256-bit algorithm set by a password key. It encrypts files by overwriting the same sectors used by the file with encrypted data, then renaming the file with a new filename extension. The CipherUSB comes new in a pass-through mode, and will not function until a password is set using the software utility.

Product Features

CAUF1W: Basic ECB 256-bit file encryption.
CAUF1W-2: Basic ECB 256-bit file encryption with Two-Factor Authentication.
CAUF1M: Basic ECB 256-bit file encryption, works with Windows or MacOS X.
CAUF1M-2: Basic ECB 256-bit file encryption, works with Windows or MacOS X and has Two-Factor Authentication.
CAUF2W: Advanced CBC 256-bit file encryption. CBC encryption adds an extra layer of complexity making the encrypted data less predictable.
CAUF2W-2: Advanced CBC 256-bit file encryption with Two-Factor Authentication.
CAUF2M: Advanced CBC 256-bit file encryption, works with Windows or MacOS X.
CAUF2M-2: Advanced CBC 256-bit file encryption with Two-Factor Authentication, works wi th Windows or MacOS X.

Two-Factor Authentication

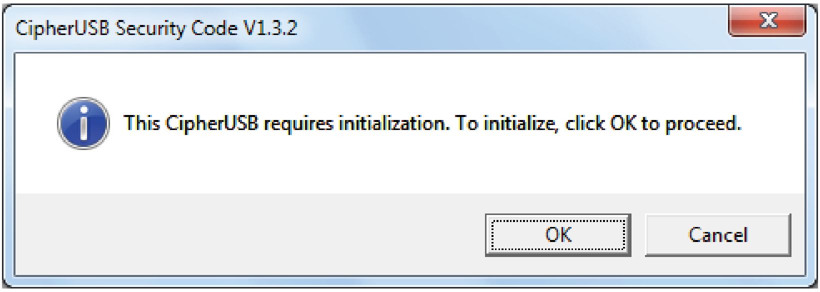
Once a CipherUSB with Two-Factor authentication (CAUF1W-2, CAUF1M-2, CAUF2W-2, CAUF2M-2) has been activated with a password, it will not allow the storage to connect to the operating system until the CipherUSB Utility has been run once and the correct password is given. The CipherUSB will only accept the password it was programmed with during the Initial Setup process. These models include an emulated CDROM Drive that will auto-start the CipherUSB Utility, which immediately prompts for the password.

Initial Setup

This procedure only needs to be done when setting up the CipherUSB for the first time, or when a new password is desired. The CipherUSB will retain the last password it was programmed with and models without Two-Factor Authentication do not require any driver or software to work.

1. Connect the CipherUSB to a computer running Windows, and connect a USB storage device into the CipherUSB. The CipherUSB will not respond until a working storage device is connected to its USB device port.

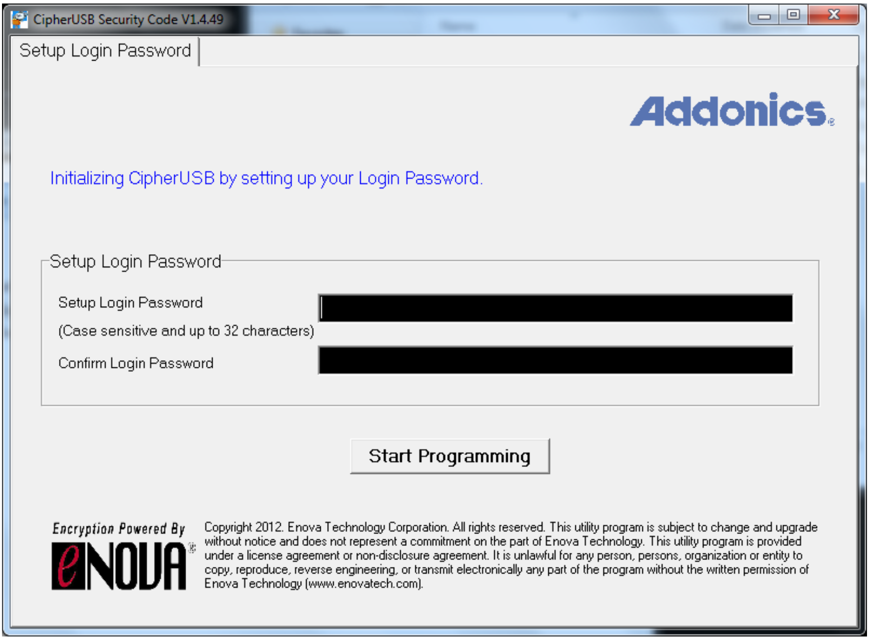
2. For models without Two-Factor Authentication, insert the CipherUSB password utility disc. If an Autorun menu appears, select "Run CipherUSB.exe" or browse to your CD drive using Windows Explorer and launch the CipherUSB program. If you are setting up the CipherUSB for the first time, the following dialog box should appear:



CipherUSB Security Code V1.3.2

This CipherUSB requires initialization. To initialize, click OK to proceed.

3. Click OK to proceed to the utility. Choose a password as short or as long (up to 32 characters) as desired, and enter it into the “Setup” and “Confirm” fields. Then click Start.



Initializing CipherUSB by setting up your Login Password.

Setup Login Password

Setup Login Password
(Case sensitive and up to 32 characters) [redacted]

Confirm Login Password [redacted]

Copyright 2012. Enova Technology Corporation. All rights reserved. This utility program is subject to change and upgrade without notice and does not represent a commitment on the part of Enova Technology. This utility program is provided under a license agreement or non-disclosure agreement. It is unlawful for any person, persons, organization or entity to copy, reproduce, reverse engineering, or transmit electronically any part of the program without the written permission of Enova Technology (www.enovatech.com).

CAUTION: KEEP YOUR PASSWORD SAFE AND REMEMBER IT. OTHER CipherUSB DEVICES CAN USE THE SAME PASSWORD TO UNLOCK MEDIA ENCRYPTED BY THIS DEVICE. IF THE PASSWORD IS LOST THE DATA IS LOST. THERE IS NO “BACK DOOR” TO UNLOCK OR RECOVER THE PASSWORD OR THE ENCRYPTION KEY.

After confirming once more for security, the CipherUSB will be programmed with a 256-bit encryption key seeded by the password. Once the CipherUSB has been programmed, a dialog will appear instructing you to remove the device and reinsert it, then the program will close automatically. After removing and reinserting the CipherUSB it will be properly initialized.

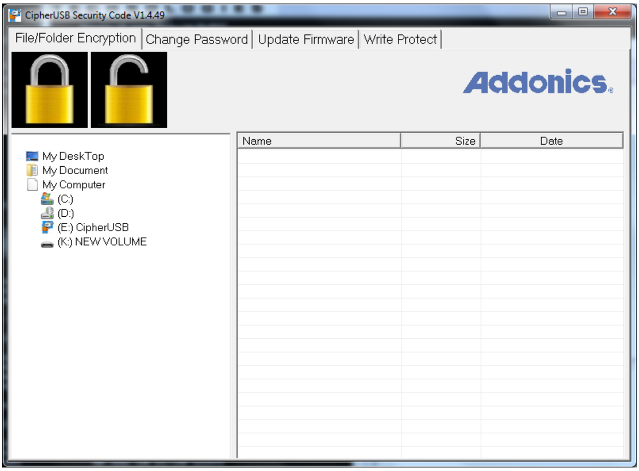
Using the CipherUSB With Storage

Data that is encrypted will only be readable after being decrypted again using a CipherUSB programmed with the correct password.

While it is required to connect the CipherUSB with a storage device attached in order to encrypt files, it is not necessary to encrypt files on the attached storage. Files may be encrypted or decrypted on any of the computer's storage devices.

Using the CipherUSB FLE To Encrypt Files

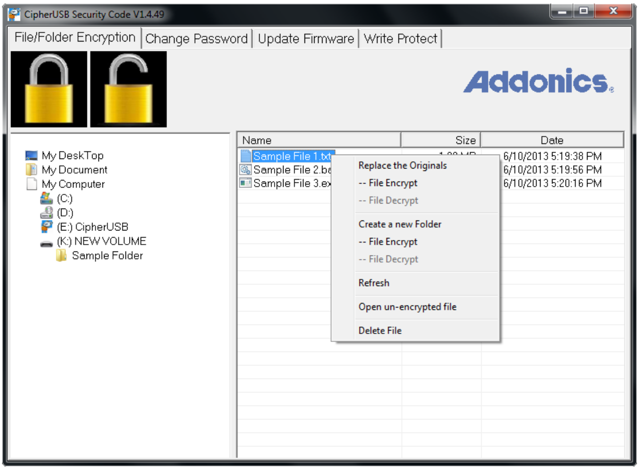
Once The CipherUSB FLE has been initialized with a password (and has been unlocked if the Two-Factor feature is included), the software will present the File/Folder Encryption screen, similar to this:



On the left side of the window is a Tree view of the computer's storage devices. Clicking on any of these will show their contents on the right side.

To encrypt files, select one or more items on the right side, then drag them to the closed padlock icon in the upper-left corner of the window. To decrypt files, select one or more encrypted files on the right side, then drag them to the open padlock icon in the upper-left corner of the window.

Alternatively, right-clicking on any selected item will bring up the context menu as shown:



Name	Size	Date
Sample File 1.txt	[illegible]	6/10/2013 5:19:38 PM
Sample File 2.ba		6/10/2013 5:19:56 PM
Sample File 3.ex		6/10/2013 5:20:16 PM

The File Encrypt and Decrypt selections in the Replace the Originals section work the same as dragging to the padlock icons.
Choosing File Encrypt in the Create a new Folder section will cause a new folder to appear called AES_Encrypted, containing the encrypted version of the files. Choosing File Decrypt in the Create a new Folder section will cause a new folder to appear called AES_Decrypt, containing the decrypted version of the files.

Performing encryption on a folder or drive will operate on all of the files in that folder or drive. Note: the encryption and decryption functions do not traverse through subfolders. Only the actual files in the selected folder or drive will be encrypted. Files located in subfolders will not be affected.

Write Protect

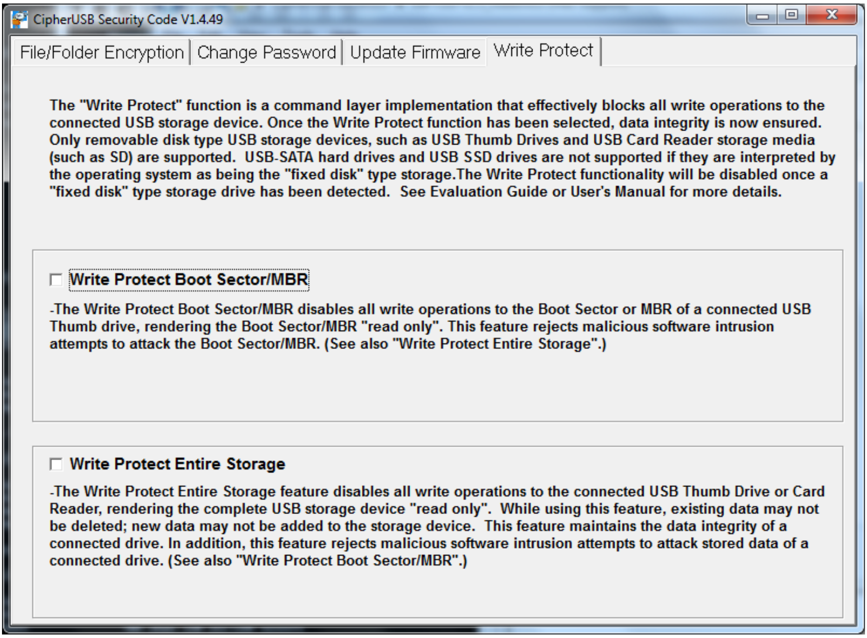
Write protection only works with storage devices that are removable media, such as USB Flash Drives or flash media in a standard reader. Write protection will not work with Fixed disk media, such as USB hard drives or SSD drives, the Addonics Pocket eSATA/USB DigiDrive, or eSATA hard disks connected through adapters such as the Addonics USB 3.0 to eSATAp Adapter or the Addonics USB 3.0 to eSATA Mini Adapter.

Write Protection works by blocking requests from the computer to write to the media and does not protect the media from being written to if the media is not connected to the CipherUSB device. It only works with the drive connected through the CipherUSB.

There are two types of Write Protection available:

Write Protect Boot Record/MBR
Checking this box will cause the CipherUSB to refuse any write requests from the computer to the first logical sector of the removable media. This feature provides basic protection against malware attacks that attempt to deploy payload at boot time or upon insertion of removable media.

Write Protect Entire Storage
Checking this box will cause the CipherUSB to refuse ALL write requests from the computer to the removable media. This feature will protect all data on the media from being erased or overwritten while in use with the CipherUSB device.



The "Write Protect" function is a command layer implementation that effectively blocks all write operations to the connected USB storage device. Once the Write Protect function has been selected, data integrity is now ensured. Only removable disk type USB storage devices, such as USB Thumb Drives and USB Card Reader storage media (such as SD) are supported. USB-SATA hard drives and USB SSD drives are not supported if they are interpreted by the operating system as being the "fixed disk" type storage.The Write Protect functionality will be disabled once a "fixed disk" type storage drive has been detected. See Evaluation Guide or User's Manual for more details.

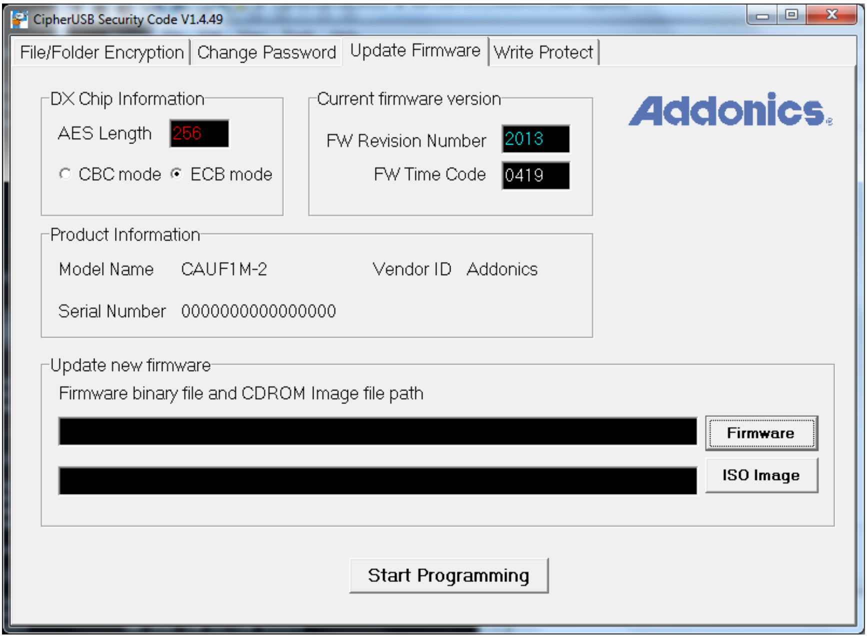
☐ Write Protect Boot Sector/MBR

-The Write Protect Boot Sector/MBR disables all write operations to the Boot Sector or MBR of a connected USB Thumb drive, rendering the Boot Sector/MBR "read only". This feature rejects malicious software intrusion attempts to attack the Boot Sector/MBR. (See also "Write Protect Entire Storage".)

☐ Write Protect Entire Storage

-The Write Protect Entire Storage feature disables all write operations to the connected USB Thumb Drive or Card Reader, rendering the complete USB storage device "read only". While using this feature, existing data may not be deleted; new data may not be added to the storage device. This feature maintains the data integrity of a connected drive. In addition, this feature rejects malicious software intrusion attempts to attack stored data of a connected drive. (See also "Write Protect Boot Sector/MBR".)

Updated Firmware



DX Chip Information

AES Length 256

○ CBC mode ● ECB mode

Current firmware version

FW Revision Number 2013

FW Time Code 0419

Product Information

Model Name CAUF1M-2 Vendor ID Addonics

Serial Number 0000000000000000

Update new firmware

Firmware binary file and CDROM Image file path

1. Read the firmware update for important changes to the unit's operation or the update procedure. If a firmware release note contradicts these instructions, follow the release notes instead.
2. Insert the CipherUSB with a storage device. The CipherUSB will not respond unless a storage device is attached to it. 3. Run the CipherUSB.exe program. If the CipherUSB unit has not been initialized with a password, the Update Firmware tab will not appear. Initialize the unit with a password, unplug it, plug it back in, then select the Update Firmware tab.
4. Be sure the DX Information section shows AES Length is 256 and ECB mode is selected for the CAUF1W, CAUF1W-2, CAUF1M-2 or CAUF1M. CBC mode for the CAUF2W, CAUF2W-2, CAUF2M, CAUF2M-2.
5. In the Update new firmware section, click the Firmware button. Change the file type to “BinaryFile(*.256) if neces sary, then browse to the folder containing the new firmware and open it.
6. Click the Start Programming button. A dialog will shortly appear instructing you to remove the CipherUSB and reinsert it. After removing and reinserting the device, the firm ware update will be completed.

NOTE: The CipherUSB may or may not need to be initialized with the password again. If a storage device using the existing password is connected when the CipherUSB is reinserted and the file system appears intact, the password has been retained. Otherwise it may be necessary to set the password again.

CONTACT US

www.addonics.com

Phone: **408-573-8580**
Fax: **408-573-8588**
Email: **http://www.addonics.com/sales/query/**